REMARKS

Claims 1-5, 71, 140, 141, 287 and 288 are pending in the above-identified application, and were rejected. With this Amendment, no claims were amended, added or cancelled. Accordingly, claims 1-5, 71, 140, 141, 287 and 288 remain at issue.

I. 35 U.S.C. § 102 Anticipation Rejection of Claims

Claims 1-4, 71, 140, and 287-288 were rejected under 35 U.S.C. § 102(b) as being anticipated by Linehan et al. (U.S. Patent No. 5,495,533). Applicants respectfully traverse this rejection.

Claim 1 is directed to a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus. The management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of the content data. The data providing apparatus provides the content data encrypted by using the content key data. The data processing apparatus decrypts the content key data and the usage control policy data stored in the key file and determines the handling of the content data based on the decrypted usage control policy data.

Linehan et al. is directed to a security system that automatically manages keys used for encryption or message authentication of data files or individual entries in databases. (See col. 6, lines 8-10.) The personal key archive security system uses two components: the Personal Key Client component on a user computer and the Personal Key Server. (See col. 6, lines 17-20.)

The Personal Key Server maintains a Personal Key Database that contains certain information required to decrypt files or check their message authentication. (See col. 7, lines 6-9.)

In Linehan et al., each data file is encrypted by the Personal Key Client at the time the file is created. (See col. 7, lines 30-33.) The Personal Key Server Database contains an entry for each file that is encrypted, and each entry contains the key used to encrypt the corresponding file, the name of the owner of the file, and the an access control list containing the names of any of the users who are permitted to access the file. (See col. 7, lines 39-45.) In Linehan et al., the access control list is not encrypted. Thus, Linehan et al. neither discloses nor suggests that the management apparatus prepares a key file storing encrypted usage control policy data indicating a content of rights such as usage permission conditions of the content data, or that the data processing apparatus decrypts the usage control policy data stored in the key file and determines the handling of the content data based on the decrypted usage control policy data, as required by claim 1.

Moreover, in Linehan et al., when a file is created, the Personal Key Client sends the ticket of the creator, along with the file's name and creation date, to the Personal Key Server. (See col. 7, lines 47-49.) The Personal Key Server generates a file encryption key, creates a new entry in the database, and responds to the Personal Key Client with the file encryption key. (See col. 7, lines 49-52.) The Personal Key Client then uses the key to encrypt the data as it is written to the file. (See col. 7, lines 52-53.)

When a file is accessed, the Personal Key Client sends the ticket of the accessor, the file's name, and the file's creation date to the Personal Key Server. (See col. 7, lines 54-57.) The

Personal Key Server retrieves the appropriate entry in the database and checks the identity of the accessor as provided in the ticket against the file owner's name and access control list in the database entry. (See col. 7, lines 57-60.) If the accessor is either the owner or one of the users named in the access control list, the Server sends the file encryption key back to the Personal Key Client. (See col. 7, lines 60-63.) The Personal Key Client uses the key to decrypt the data as it is read from the file. (See col. 7, lines 63-64.) Thus, in Linehan et al., the Personal Key Server that generates the file encryption key and maintains the Personal Key Server Database does not store the encrypted file. Accordingly, Linehan et al. does not disclose or suggest a management apparatus that prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data, as required by claim 1.

For all of the reasons indicated above, Applicants respectfully submit that claim 1, and claims 2-4 that depend from claim 1, are allowable over Linehan et al. For reasons similar to those discussed regarding claim 1, Applicants respectfully submit that claims 71, 140 and 287-288 are also allowable over Linehan et al. Accordingly, Applicants respectfully request withdrawal of this rejection.

II. 35 U.S.C. § 103 Obviousness Rejection of Claims

Claims 5 and 141 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Linehan et al. (U.S. Patent No. 5,495,533) in view of Kravitz et al. (U.S. Patent No. 6,738,905). Applicants respectfully traverse this rejection.

As discussed above, Linehan et al. neither discloses nor suggests that the management apparatus prepares a key file storing encrypted usage control policy data indicating a content of rights such as usage permission conditions of the content data, or that the data processing apparatus decrypts the usage control policy data stored in the key file and determines the handling of the content data based on the decrypted usage control policy data. Moreover, Linehan et al. does not disclose or suggest a management apparatus that prepares a key file storing encrypted content key data and encrypted usage control policy data indicating a content of rights such as usage permission conditions of said content data. Thus, it would not have been obvious to one skilled in the art at the time of the invention to modify Linehan et al. with the disclosure of Kravitz et al. to derive claim 5 or claim 141, both of which include these limitations. Accordingly, Applicants respectfully request withdrawal of this rejection.

III. Conclusion

In view of the above amendments and remarks, Applicants submit that all claims are clearly allowable over the cited prior art, and respectfully request early and favorable notification to that effect.

Respectfully submitted,

Dated: December 23, 2005

By: _____

Marina N. Saito
Registration No. 42,121
SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(312) 876-8000